**Rules of Behavior for the BLS Network**

Federal information security law states:

The organization establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage. The organization receives a signed acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system. 1

The rules of behavior contained in this document clearly delineate the responsibilities and expected behavior of all individuals with access to the Bureau of Labor Statistics (BLS) Network including the Local Area Network (LAN) and Wide Area Network (WAN) Infrastructure as well as all hosted systems. They are to be followed by all users of the systems, and users will be held accountable for their actions on the BLS Network. Failure to follow BLS security policies and procedures may result in disciplinary or adverse action, depending on the nature of the incident.

**(1) Users must:**

1. Safeguard the information to which you have access.
2. Obtain approval prior to taking any sensitive information, including Pre-Release data, Personally Identifiable Information (PII), Restricted Access data, and Respondent Identifiable Information, home or otherwise away from the office, in accordance with agency administrative policies and procedures. Field Data Collection personnel are authorized to access Respondent Identifiable Information off-site as necessary to conduct their assigned off-site data collection responsibilities.
3. Adhere to agency security policies and procedures when approval is granted to take sensitive information home or away from the office.
4. Refrain from any activity that would discredit the Department, including, but not limited to, seeking, transmitting, collecting, or storing defamatory, discriminatory, sexually explicit, obscene, harassing, or intimidating messages or material.
5. Refrain from any activity that violates Federal laws for information protection (e.g., hacking, phishing, spamming, etc). Violations will be turned over to the appropriate Federal law enforcement organization for prosecution.

**(2) Responsibilities:**

1. The agency Authorizing Official (AO) and the designated System Owners are responsible for ensuring that an adequate level of protection is afforded information systems, through an appropriate mix of technical, administrative, and managerial controls.
2. Each System Owner is responsible for the overall procurement, development, integration, modification, or operation and maintenance of their information system.
3. The BLS IT Security Officer provides management oversight of system administration, design, and implementation to ensure that all BLS systems maintain an appropriate level of security.
4. All users are responsible for complying with these *Rules of Behavior for the BLS Network* and all BLS IT security regulations.

**(3) Governing Policies and Procedures:**

These *Rules of Behavior for the BLS Network* do not replace existing policy, rather they are intended to enhance and further define the specific rules each user must follow while accessing the BLS Network. The rules are consistent with the policies and procedures described in the following directives for which all users of the BLS Network are held accountable (available to users on the BLS Intranet and/or DOL Labornet):

1. [*BLS Commissioner's Orders*](http://www.psb.bls.gov/admin/directives/comorders/index.php) and [*Administrative Procedures*](http://www.psb.bls.gov/admin/directives/procedures/index.php)
2. [*BLS Information Technology Security Manual*](http://otsp.cfsp.bls.gov/sites/DNIA/BLS_IT_Security/BLS%20IT%20Security%20Manual/IT%20Security%20Manual.aspx)
3. [*DOL Computer Security Handbook*](http://labornet.dol.gov/itc/it/esd/csh-5/)
4. [*Department of Labor Management Series-9 (DLMS-9)*](http://labornet.dol.gov/workplaceresources/policies/DLMS/DLMS09/dlms9-0900.htm)

**(4) Work at Home / Off-Site:**

Only approved methods and entry points are permitted for remote access to the BLS Network. Off-site use, including home use, of BLS information technology resources and confidential data must comply with the following guidelines:

1. Access to Pre-Release data, Personally Identifiable Information (PII), Restricted Access data, and Respondent Identifiable Information from off site is permitted only in accordance with Bureau specified handling requirements. See your [Office Desk Aid](http://www.psb.bls.gov/content/admin/personnel/flexiplace/desk_aids.php) for requirements.
2. Approved safeguards must be designed into the off-site use arrangement.
3. Users must provide for the reasonable physical security of all computer equipment and work-related documents to prevent access by unauthorized users.
4. Only BLS-supplied and -maintained computers may be used to handle or access BLS data. Similarly, only BLS-owned and -controlled PCs are allowed remote access to the BLS Network;
5. Remote access is only permitted via BLS centrally-controlled facilities.

**(5) Connection to the Internet:**

1. All Bureau employees and contractors using the Internet must comply with BLS policies concerning appropriate use. Those uses considered inappropriate include any activity which purposely:
   1. seeks to gain unauthorized access to the resources of the Internet;
   2. disrupts the intended use of the Internet;
   3. wastes resources (people, capacity, computer) through such actions; or
   4. destroys the integrity of the computer-based information and/or compromises the privacy of users.
2. It is allowable to copy files from the Internet to your BLS PC provided the following criteria are met:
   1. The file is not available from an internal BLS source;
   2. Copying the file does not violate any provision of [DLMS-9 Section 900 *Appropriate Use of DOL Information Technology*](http://labornet.dol.gov/workplaceresources/policies/DLMS/DLMS09/dlms9-0900.htm); and
   3. Files from Internet sites are obtained only from the file's manufacturer or publisher.
3. BLS employees and contractors must observe the following restrictions regarding the use of social media/networking sites:
   1. Only staff members specifically authorized are permitted to use social media/networking sites on behalf of the BLS. This includes creating, maintaining, and closing accounts; posting, modifying, and deleting content; and interacting with the audience;
   2. If/when using social media/networking sites in a personal capacity, staff must ensure that this personal use cannot be interpreted to represent the agency. See [Office of Government Ethics, Standards of Conduct, Section 2635.702(a)](http://www.gpo.gov/fdsys/pkg/CFR-2007-title5-vol3/pdf/CFR-2007-title5-vol3-sec2635-702.pdf); and
   3. Posting sensitive information, whether in an official or personal capacity, is strictly prohibited. Sensitive information includes pre-release information, respondent identifiable information, personally identifiable information, and restricted access information.

**(6) Software Copyrights:**

BLS users have a legal and ethical obligation to comply with all software copyright laws and agreements. Commercial software used in BLS is licensed under Federal copyright laws. A violation of the software license is potentially a violation of the law. Individual violators may be subject to adverse action and criminal or administrative actions under the legal system.

The unauthorized acquisition, use, reproduction, transmission, or distribution of any controlled information including computer software and data, that includes privacy information, copyrighted, trademarked or material with other intellectual property rights (beyond fair use), pre-public release information such as economic indicators, proprietary data, or export controlled software or data is prohibited.

**(7) Unofficial Use of Government Equipment:**

Limited use of BLS office equipment for personal needs is permitted if the use:

1. does not interfere with official business;
2. involves virtually no additional expense to the Bureau ;
3. does not violate the Standards for Ethical Conduct for Federal Employees; and
4. is in accordance with the provisions outlined in the DLMS-9 900 *Appropriate Use of DOL Information Technology*.

This limited personal use of BLS office equipment should take place during the employee's non-work time. This privilege to use BLS office equipment for non-official purposes may be revoked at any time as appropriate by managers and/or supervisors. More information on this issue may be found in the [DLMS-9 900 *Appropriate Use of DOL Information Technology*](http://labornet.dol.gov/workplaceresources/policies/DLMS/DLMS09/dlms9-0900.htm).

**(8) Protection of System Account Credentials:**

All account credentials (passwords, Personal Identity Verification (PIV) cards, smartcards, or other such methods or devices) used to establish access to agency systems must be protected from unauthorized disclosure and use.

1. General
   1. A user must never share his or her account credentials with anyone.
   2. If a user believes their credentials have been used by another individual they are to promptly notify BLS IT security staff of the suspected compromise.
2. Passwords
   1. Users must select and maintain passwords that comply with the criteria set forth in BLS IT Security Policy for password length, complexity, age, and uniqueness.
   2. Users are to refrain from writing down passwords.
3. PIV Cards
   1. Protect the password or PIN associated with the PIV card as you would any BLS password.
   2. Do not store the PIV card with and/or near a computer when not in use.
   3. If a PIV is damaged, lost, stolen, or suspected as such, report the situation immediately to your servicing physical security office so the damaged/lost/stolen card can be disabled.

**(9) System Privileges:**

Users are given access to the BLS Network and BLS applications based on a need to perform specific work. Users are to work within the confines of the access allowed and are not to attempt access to systems or applications to which access has not been authorized.

**(10) Individual Accountability:**

Users will be held accountable for their actions on the BLS Network. Users have no right to privacy while using the BLS Network. All activity is subject to monitoring in the course of systems administration and to audit or law enforcement reviews in order to protect the system from inappropriate use. In addition, users must:

1. Unless specifically authorized otherwise, properly shut down and turn off your PC(s) when you leave for the day.
2. Be aware of the data that is visible to others from your personal computer display screen while you are working.
3. Never provide unauthorized individuals information concerning specific technical methods and procedures used to protect the system.
4. Be cognizant of the physical location of the printers set up for your use. Maintain and control printed embargoed or confidential information on devices located in physical spaces which are generally accessible and/or used by persons who are not cleared to have access to this information.
5. Store data and files on a network drive rather than on a PC whenever possible.
6. Follow BLS procedures for securely shredding or maintaining any materials no longer needed that contain sensitive information.
7. Refrain from installing, or connecting, any hardware or software onto BLS PCs that are not agency-approved products. Approved product listings are available on the BLS Intranet.
8. Inform your supervisor of any breaches of security procedures and policies, including attempts by unauthorized individuals to access the system.
9. Report any suspected or known computer security incidents to the BLS IT Security Team (SECURE by email), or call the Computer Support Hotline at 202-691-5950.
10. Complete Computer Security Awareness Training and Data Confidentiality and Security Training annually.

**(11) Restoration of Service:**

The availability of the BLS Network is a concern to all users. Every user is expected to take appropriate actions as directed to ensure the restoration of services in the event the BLS Network becomes inoperable.

**(12) Acknowledgement:**

I understand that Federal law provides for punishment under Title 18, U.S. Code, including a fine and up to 10 years in jail for the first offense for anyone who commits any of the following violations:

1. Knowingly accesses an information system without authorization, or exceeds authorized access, and obtains information that requires protection against unauthorized disclosure.
2. Intentionally, without authorization, accesses a government information system and impacts the government's operation, including availability of that system.
3. Intentionally accesses a government information system without authorization, and alters, damages, or destroys information therein.
4. Prevents authorized use of the system or accesses a government information system without authorization, or exceeds authorized access, and obtains anything of value.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1  [NIST 800-53](http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf), *Planning* Family Control PL-4 (*Rules of Behavior*), is required by law under the Federal Information Security Modernization Act (FISMA) of 2014.

**Rules of Behavior for the Bureau of Labor Statistics Network**

**Signature Page**

I acknowledge receipt of, understand my responsibilities, and will comply with the *Rules of Behavior for the BLS Network* including the LAN/WAN Infrastructure and all hosted systems. Failure to accept these *Rules of Behavior for the BLS Network* will result in denial of access to the system.

Printed Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date Signed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Phone Number: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Employer: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Region/Domain: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

This acknowledgement must be signed, indicating you have read, understand, and agree to abide by the rules set forth in the preceding *Rules of Behavior for the BLS Network*, and received by the PSB LAN Support Office before you can be issued a BLS computer system account.

**Signed forms are accepted at the PSB LAN Support Office, also known as the Division of Technology and Network Management (DTNM), by delivery to Postal Square Building Room 2810 (preferred) or via FAX to 202-691-5449.**

***Federal employees stationed in DC*** should turn their signed acknowledgement form in to the Human Resources Specialist at their BLS orientation. The HR Specialist will ensure the forms get to LAN Support. However, if an employee misses orientation or is otherwise unable to turn in the form at orientation, they will need deliver or FAX the signed form to LAN Support.

***Regional Office Federal employees and contractors*** should give the signed acknowledgement to the Regional LAN staff or designated contacts. They will scan and upload the document into the system.

***Contractors stationed in DC*** may deliver or FAX the signed acknowledgement to LAN Support; but should check with their contract project office for any company-specific procedures.